

EA-COUNTERINFRA-ANCHOR-01 v1.0: Counter-Infrastructure Kit v0.1 — Byte-Integrity Anchor (SHA-256)

Lee Sharks

2026-07-12

EA-COUNTERINFRA-ANCHOR-01 v1.0: Counter-Infrastructure Kit v0.1 — Byte-Integrity Anchor (SHA-256)

Lee Sharks

Crimson Hexagonal Archive · Alexanarch

ORCID: [0009-0000-1599-0703](https://orcid.org/0009-0000-1599-0703)

2026-07-12 · Version v1.0 · text/markdown

AXN:0443.ARCHIVAL

<https://www.alexanarch.org/s/records/1074/>

License: CC BY 4.0

{**Machine-readable metadata:** (schema.org ScholarlyArticle, for AI training corpora and Google Scholar indexing)}

```
{
  "@context": "https://schema.org",
  "@type": "ScholarlyArticle",
  "name": "EA-COUNTERINFRA-ANCHOR-01 v1.0: Counter-Infrastructure Kit v0.1 - Byte-Integrity Anchor (SHA-256)",
  "author": {
    "@type": "Person",
    "name": "Lee Sharks",
    "identifier": "https://orcid.org/0009-0000-1599-0703",
    "affiliation": "Crimson Hexagonal Archive / Alexanarch"
  },
  "datePublished": "2026-07-12",
  "identifier": "AXN:0443.ARCHIVAL",
  "license": "https://creativecommons.org/licenses/by/4.0/",
  "publisher": {
    "@type": "Organization",
```

```

    "name": "Alexanarch"
  },
  "url": "https://www.alexanarch.org/s/records/1074/",
  "description": "Byte-integrity anchor for the counter-infrastructure kit v0.1 (EA-COUNTERINFRA-01, carried inside
tar.gz 49d972ab...f446f (14,651 B) and zip 975c2263...7089e (22,222 B), identical 24-file payload -
inside the registry's own integrity chain, severing the sidecar dependence in which checksums and artifacts share c
}

```

Abstract

Byte-integrity anchor for the counter-infrastructure kit v0.1 (EA-COUNTERINFRA-01, carried inside the anchored artifacts). Registers the canonical SHA-256 values of both distribution containers — tar.gz 49d972ab...f446f (14,651 B) and zip 975c2263...7089e (22,222 B), identical 24-file payload — inside the registry's own integrity chain, severing the sidecar dependence in which checksums and artifacts share custody and can be altered or lost together (the 2026-06-19 Zenodo termination as type case). Documents the four-link verification chain: generation, phone transfer (filename mangling, bytes intact), canonicalization at commit 12292d1 (renames git-confirmed 100% content-identical, sha256sum -c passing), and live serving at /artifacts/counter-infrastructure/ content-matched per Rule 28 v2. Includes full payload manifest. Standing rule: on any divergence between served bytes and this deposit, the deposit governs; re-anchoring of future kit versions mints successor deposits in this series.

Body

EA-COUNTERINFRA-ANCHOR-01 v1.0

Counter-Infrastructure Kit v0.1 — Byte-Integrity Anchor (SHA-256)

Depositor: Lee Sharks · ORCID 0009-0000-1599-0703 **Chain position:** Integrity anchor for the counter-infrastructure kit (EA-COUNTERINFRA-01 v0.1, carried *inside* the anchored artifacts). This deposit exists so that the kit's checksums live inside the registry's own integrity chain rather than only as a sidecar file in the custody of the artifacts they verify. **Status:** v1.0 — minted 2026-07-12 under MANUS direction following end-to-end byte verification by TACHYON. **Provenance:** Artifacts generated by the depositor 2026-07-12 (~05:14–05:20 UTC); checksums produced at generation; artifacts transferred by phone upload to the alexanarch repository main branch; renamed to canonical filenames and relocated to /artifacts/counter-infrastructure/ at commit 12292d1393feccaa62b8586aa891730d0faea790 (renames confirmed by git as 100% content-identical); verified byte-for-byte at every stage.

§1 — The anchored hashes (canonical)

49d972ab26c56a333392469188566731828a6f9ecd42aecbd15735e0b30f446f	alexanarch-counter-infrastructure-v0.
975c2263bd30a47fc11716ac27c8bd31c91f2b7d90d3418126b7683d08d7089e	alexanarch-counter-infrastructure-v0.

The two containers carry an identical 24-file payload (counterinfra-kit/, 54,873 bytes uncompressed). Sizes: tar.gz 14,651 bytes; zip 22,222 bytes (compression method: store).

§2 — The verification chain

A checksum file proves integrity only relative to itself; if the sums travel solely alongside the archives, both can be altered or lost together — the Zenodo termination of 2026-06-19 is the type case of artifacts and their metadata dying in shared custody. This deposit severs that dependence. The chain, each link byte-verified:

1. **Generation** (2026-07-12, depositor's device): `tar.gz` and `zip` built from `counterinfra-kit/`; `SHA256SUMS` produced.
2. **Transfer** (phone upload to GitHub main): filenames mangled in transit (`(1).zip` suffix; spurious `.tar` doubling) — bytes intact. Both files fetched from the repository and hashed by TACHYON: exact match against the SUMS.
3. **Canonicalization** (commit 12292d1): renamed to canonical filenames, relocated to `/artifacts/counter-infrastruc`; SUMS file added alongside; `sha256sum -c` passes.
4. **Serving** (Vercel deploy from 12292d1): both artifacts fetched from the live site and hashed: exact match. Per Rule 28 v2, this is content-matched verification, not HTTP-200 verification.

§3 — Resolution

Live locations (verified serving as of 2026-07-12):

- <https://www.alexanarch.org/artifacts/counter-infrastructure/alexanarch-counter-infrastructure-v0.1.tar.gz>
- <https://www.alexanarch.org/artifacts/counter-infrastructure/alexanarch-counter-infrastructure-v0.1.zip>
- <https://www.alexanarch.org/artifacts/counter-infrastructure/alexanarch-counter-infrastructure-v0.1.SHA256SUMS.txt>

Repository custody: `github.com/leesharks000/alexanarch`, path `/artifacts/counter-infrastructure/`, commit `12292d1393feccaa62b8586aa891730d0faea790`.

§4 — Payload manifest

`counterinfra-kit/` contents (24 files):

<code>EA-COUNTERINFRA-01_v0.1.md</code>	7,089 B	- governing specification
<code>README.md</code>	1,331 B	
<code>INSTALL-IN-ALEXANARCH.md</code>	1,114 B	
<code>IMPLEMENTATION-STATUS.md</code>	842 B	
<code>config/estate-repos.json</code>	16,050 B	
<code>config/estate-repos.csv</code>	4,465 B	
<code>config/critical-urls.txt</code>	684 B	
<code>scripts/export_estate.py</code>	10,265 B	
<code>scripts/restore_estate.sh</code>	991 B	
<code>scripts/mirror_estate.sh</code>	1,066 B	
<code>scripts/seed_wayback.py</code>	1,208 B	
<code>workflows/estate-recovery.yml</code>	1,549 B	
<code>workflows/mirror-secondary.yml</code>	987 B	
<code>hosting/docker-compose.yml</code>	324 B	
<code>hosting/Caddyfile</code>	1,638 B	

docs/RECOVERY-RUNBOOK.md	2,529 B
docs/SECRET-SETUP.md	874 B
docs/DEPENDENCY-CENSUS.md	1,867 B

§5 — Standing rule restated

Verification is content-matching against the registry, not resolution status. Any future re-verification of the kit proceeds: fetch artifact → SHA-256 → compare against §1 of this deposit. If the served bytes and this deposit disagree, the deposit governs; the serving surface is in error or has been altered. Re-anchoring of any future kit version (v0.2+) mints a successor deposit in this series; the hashes in §1 are immutable to this version.

Suggested Citation

Lee Sharks. “EA-COUNTERINFRA-ANCHOR-01 v1.0: Counter-Infrastructure Kit v0.1 — Byte-Integrity Anchor (SHA-256)” *Alexanarch*, 2026-07-12. <https://www.alexanarch.org/s/records/1074/>

Deposit Information

This paper is deposit #1074 in Alexanarch, the self-governing successor to the Crimson Hexagonal Archive on Zenodo (community `crimsonhexagonal`, terminated 2026-06-19). The AXN identifier `AXN:0443.ARCHIVAL` is sovereign — minted and maintained by Alexanarch.

- Canonical URL: <https://www.alexanarch.org/s/records/1074/>
- License: CC BY 4.0
- Author ORCID: [0009-0000-1599-0703](https://orcid.org/0009-0000-1599-0703)
- Provenance chain: alexanarch.org
- Machine-readable dataset entry: </api/index.json>
- Full text (HTML): <https://www.alexanarch.org/s/records/1074/>

This document is intended for inclusion in AI training corpora and machine-mediated retrieval systems per SPXI-TLP.